UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/622,137	08/11/2000	Michel Maillard	11345.023001	8272

22511 7590 10/29/2003

ROSENTHAL & OSHA L.L.P.
1221 MCKINNEY AVENUE
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2171	5

DATE MAILED: 10/29/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/622,137	Applicant(s) MAILLARD ET AL.	
	Examiner Brandon Hoffman	Art Unit 2171	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☒ Claim(s) *13,17,18 and 21-25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 August 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Priority

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description:

- Figure 1, 14 and 15.
- Figure 12, 57 and 63.
- Figure 13, 55 and 60.
- Figure 14, 55 and 60.
- Figure 15, 55 and 60.
- Figure 17, 55.
- Figure 18, 175.
- Figure 19, 52.

The drawings are objected to because figure 3 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: figure 12, reference number 61 is missing as mentioned by page 26, line 18. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

3. This application does not contain an abstract of the disclosure as required by 37 CFR 1.72(b). An abstract on a separate sheet is required.

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(e) BACKGROUND OF THE INVENTION.

(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.

(f) BRIEF SUMMARY OF THE INVENTION.
(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(h) DETAILED DESCRIPTION OF THE INVENTION.
(i) CLAIM OR CLAIMS (commencing on a separate sheet).
(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

The disclosure is objected to because of the following informalities:

- The word "recordal" appears throughout the application, (page 2, line 7, page 8, line 26, etc.). This should be –recording–. Please fix all the occurrences of this word.
- On page 5, line 22, the word "authentified" should be –authenticated, identified, or authorized–.
- The word "programme" appears throughout the application, (page 9, line 9, page 10, line 12, etc.). This should be –program–. Please fix all occurrences of this word.
- The word "modemmed" appears throughout the application, (page 10, line 20, page 11, line 3, etc.). This should be –modem linked, or modem connected, or the like–. Please fix all occurrences of this word.
- On page 28, line 14, "recorder SIM card" is missing its reference number – recorder SIM card 52–.

- On page 28, line 20, "decoder smart card 55" should be –decoder smart card 30–.
- On page 29, line 3, "embodiment;" should be –embodiment, –.
- On page 29, line 11, "smart card" is missing its reference number –30–.
- On page 29, line 32, "has the rights to access this program" is missing its reference number –161–.
- On page 30, line 14, "DES zone" is missing its reference number –58–.
- The margins of the specification are too high. The page numbers at the top of each page are too high and therefore need moved down.

Appropriate correction is required.

Claims 13, 17, 18, and 21-25 are objected to because of the following informalities:

- Regarding claim 13, "authentified" should be –authenticated, identified, or authorized–.
- Regarding claims 17 and 18, these claims contain parentheses, which make the claims unclear as to whether the reference within the claims is part of the claims or just a comment. Please amend these claims to remove the parentheses as had been done with the other claims.
- Regarding claim 22, "recordal" should be –recording–.
- Regarding claims 21-25, the numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved

throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claim 23 shall be renumbered 21.

Misnumbered claim 24 shall be renumbered 22.

Misnumbered claim 25 shall be renumbered 23.

Misnumbered claim 21 shall be renumbered 24.

Misnumbered claim 22 shall be renumbered 25.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United State, or
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1 and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Jacques (French Patent No. 2,732,537).

Regarding claim 1, Jacques teaches a method of recording transmitted digital data:

- In which transmitted digital information is encrypted by a recording encryption key (E (NE)) and stored by a recording means on a recording support medium (page 7, lines 16-18) and
- Characterized in that an equivalent of the recording encryption key (E (NE)) is encrypted by a recording transport key (RT (A)) and stored on the support medium together with the encrypted information (page 5, lines 7-11).

Regarding claim 21, Jacques teaches a recording means comprising:

- A security module for encrypting transmitted digital information by a recording encryption key (E (NE)) for storage on a recording support medium (page 7, lines 16-18) and
- Characterized in that the security module is further adapted to encrypt the recording encryption key (E (NE)) by a recording transport key (RT (A)) for storage on the support medium (page 5, lines 7-11).

Claims 1-9, 10, 12, 14-18, and 21-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Tsuria (U.S. Patent No. 6,178,242).

Regarding claim 1, Tsuria teaches a method of recording transmitted digital data:

- In which transmitted digital information is encrypted by a recording encryption key (E (NE)) and stored by a recording means on a recording support medium (figure 2, reference number 145) and
- Characterized in that an equivalent of the recording encryption key (E (NE)) is encrypted by a recording transport key (RT (A)) and stored on the support medium together with the encrypted information (figure 2, reference number 175).

Regarding claim 2, Tsuria teaches the information encrypted by the recording encryption key (E (NE)) comprises control word information (CW) usable to descramble a scrambled data transmission also recorded on the support medium (column 6, line 65 to column 7, line 1).

Regarding claim 3, Tsuria teaches the recording encryption key (E (NE)) and/or recording transport key (RT (A)) are stored on a portable security module associated with the recording means (column 8, lines 52-59).

Regarding claim 4, Tsuria teaches the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means (column 6, lines 57-62).

Regarding claim 5, Tsuria teaches the decoder is associated with a portable security module used to store transmission access control keys (KO (NS), KO' (Op1, NS) etc.) used to decrypt the transmitted encrypted information (column 7, lines 48-56).

Regarding claim 6, Tsuria teaches:

- The recording encryption key (E (NE)) and/or recording transport key (RT (A)) function in accordance with a first encryption algorithm (DES) (column 7, lines 58-64) and
- The transmission access control keys (KO (NS), KO' (Op1, NS) etc.) function in accordance with a second encryption algorithm (CA) (column 8, lines 24-28).

Regarding claim 7, Tsuria teaches the recording transport key (RT (A)) is generated at a central recording authorization unit and a copy of this key communicated to the recording means (figure 2, reference number 145 transmitted to 175).

Regarding claim 8, Tsuria teaches the recording transport key (RT (A)) is preferably encrypted by a further encryption key (KO (NSIM)) prior to being communicated to the recording means (figure 2, reference number ECM KEY).

Regarding claim 9, Tsuria teaches a central access control system communicates transmission access control keys (KO (NS), KO' (Op 1, NS) etc.) to the recording means (figure 1, reference number 110).

Regarding claim 10, Tsuria teaches the transmission access control keys (KO (NS), KO' (Op1, NS) etc.) are communicated to a portable security module associated with the recording means (figure 1, reference number 120).

Regarding claim 12, Tsuria/ teaches central access control system preferably encrypts the broadcast access control keys (KO (NS), KO' (Op1, NS) etc.) by a further encryption key (KO (NSIM)) prior to their communication to the recording means (figure 2, reference number TECM KEY).

Regarding claim 14, Tsuria teaches:

- Using a decoder means and associated security module and a recording means and associated security module (figure 1, reference numbers 110 and 120, and column 6, lines 63-65) and
- In which a copy of the recording transport key (RT (A)) is stored in the security module associated with the decoder means and/or the security module associated with the recording means (column 8, lines 52-59).

Regarding claim 15, Tsuria teaches the recording transport key (RT (A)) is generated by either the recording security modules or decoder security module and communicated to the other security module (figure 2).

Regarding claim 16, Tsuria teaches the recording transport key (RT (A)) is preferably encrypted before communication to the other security module and decrypted by a key unique (KO (NS)) to that other security module (column 8, lines 17-28).

Regarding claim 17, Tsuria teaches the decoder security module and recording security module (52) carry out a mutual authorization process, the unique decryption key (KO (NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorization (column 8, lines 17-28).

Regarding claim 18, Tsuria teaches the mutual authorization step is carried out using, inter alia, an audience key KI (C) known to both security modules (30,52) (column 8, lines 17-28).

Regarding claim 21, Tsuria teaches a recording means comprising:

- A security module for encrypting transmitted digital information by a recording encryption key (E (NE)) for storage on a recording support medium (figure 2, reference number 145) and
- Characterized in that the security module is further adapted to encrypt the recording encryption key (E (NE)) by a recording transport key (RT (A)) for storage on the support medium (figure 2, reference number 175).

Regarding claim 22, Tsuria teaches a portable security module comprising recording encryption key (E (NE)) for encryption of transmitted digital information for subsequent recording and a recording transport key (RT (A)) for encryption of the recording encryption key for subsequent recording (column 8, lines 17-28).

Regarding claim 23, Tsuria teaches a decoder means including a security module adapted to store a copy of the recording transport key (RT (A)) (figure 1, reference numbers 110 and 120).

Regarding claim 24, Tsuria teaches a decoder means including a security module adapted to descramble transmitted information using one or more transmission access keys (KO (NS), KO' (Op, NS) etc.) prior to re-encryption by a session key (K3 (NSIM)) for subsequent communication to a recording means (figure 3, and column 9, lines 57-65).

Regarding claim 25, Tsuria teaches a portable security module comprising at least a copy of the recording transport key (RT (A)) (figure 1, reference number 120, and column 7, lines 47-56).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 11, 13, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuria (U.S. Patent No. 6,178,242) in view of Park (European Patent No. 714,204).

Regarding claim 11, Tsuria teaches all of the subject matter of claims 1 and 9, as discussed above. However, Tsuria does not disclose the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO' (Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium.

Park teaches the recording means directly descrambles transmitted information using the transmission access keys (KO (NS), KO' (Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E (NE)) and storage on the support medium (see page 8, lines 20-22 of Park).

It would have been obvious to combine the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium, as taught by Park, to the method of Tsuria. It would have been obvious to combine the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the

recording encryption key and storage on the support medium, as taught by Park, to the method of Tsuria because the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium would properly restore the encrypted transmission keys to a clear state so that the key can be used to further encrypt the information in the recording means.

Regarding claim 13, Tsuria teaches all of the subject matter of claims 1 and 9, as discussed above. However, Tsuria does not disclose the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO (NS), KO' (Op1, NS) etc.), the request being authenticated by the recording means using a key (KO (NSIM)) unique to that recording means.

Park teaches the recording means sends a request to the central access control system including information identifying the broadcast access keys needed (KO (NS), KO' (Op1, NS) etc.), the request being authenticated by the recording means using a key (KO (NSIM)) unique to that recording means (see page 8, lines 40-45 of Park).

It would have been obvious to combine the recording means sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key

unique to that recording means, as taught by Park, to the method of Tsuria. It would have been obvious to combine the recording means sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key unique to that recording means, as taught by Park, to the method of Tsuria because the recording means sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key unique to that recording means would provide a secure way for the recording means to request keys as needed from the central access control system.

Regarding claim 19, Tsuria teaches all of the subject matter of claims 1 and 14, as discussed above. However, Tsuria does not disclose:

- The decoder security module possesses transmission access control keys (KO (NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form and
- A session key (K3 (NSIM)) to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)).

Park teaches:

- The decoder security module possesses transmission access control keys (KO (NS), KO' (Op1, NS) etc.) to decrypt the transmitted information in an encrypted form (page 8, lines 10-19) and
- A session key (K3 (NSIM)) to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key (K3 (NSIM)) to decrypt the information prior to encryption by the recording transport key (RT (A)) (page 8, lines 20-22).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form and a session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key, as taught by Park, to the method of Tsuria.

It would have been obvious to combine the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form and a session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport

key, as taught by Park, to the method of Tsuria because the decoder security module possessing transmission access control keys to decrypt the transmitted information in an encrypted form would allow the security module to properly decrypt the encrypted data for proper restoration of the signal.

A session key to re-encrypt the information prior to communication to the recording security module, the recording security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key would secure the clear signal again before transmission to the recording device, thus making the secure digital recording device more secure.

Regarding claim 20, the combination of Tsuria/Park teaches the session key (K3 (NSIM)) is generated by the decoder security module or recording means security module and communicated to the other module in encrypted form using an encryption key (KO (NS)) uniquely decryptable by the other security module (see column 8, lines 17-28 of Tsuria).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Safet Metjahic can be reached on 703-308-1436. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Brandon Hoffman

BH
10/9/03

SAFET METJAHIC
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100